Free and Open Source Software Conference

Apple OS X und iOS Management

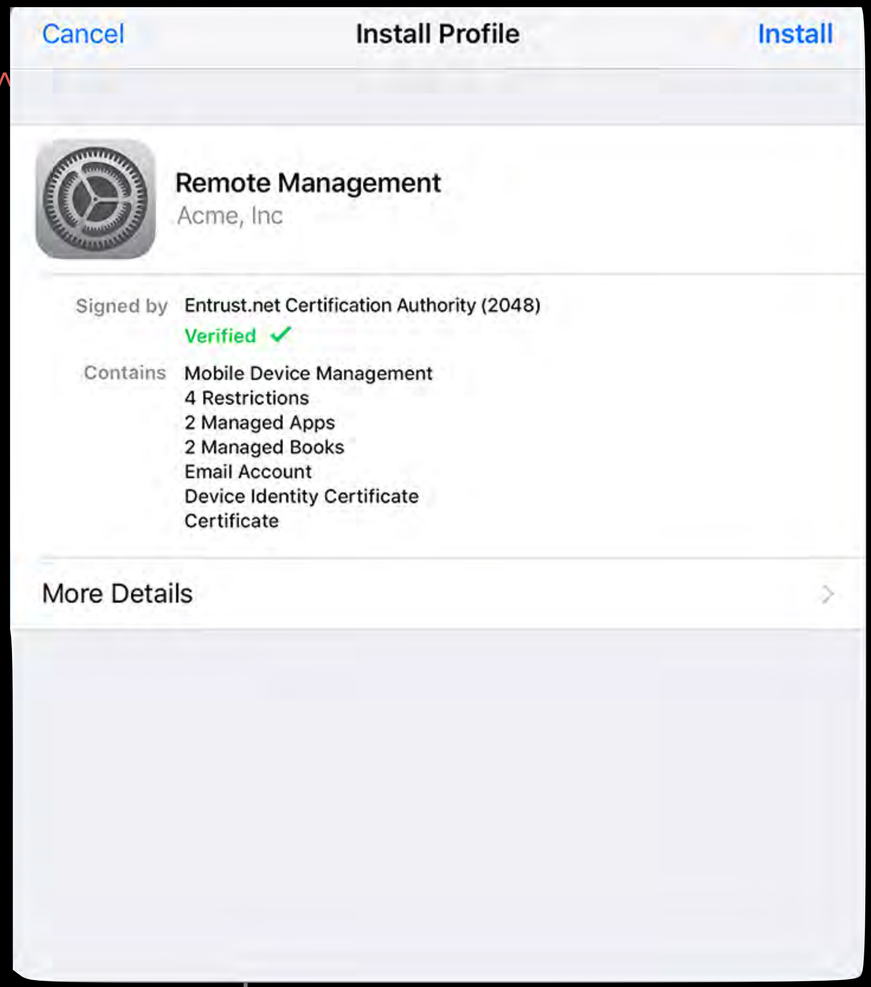
UNIVERSITY OF OXFORD

Managing Mobile Devices running iOS

Configuration Profiles

UNIVERSITY OF OXFORD

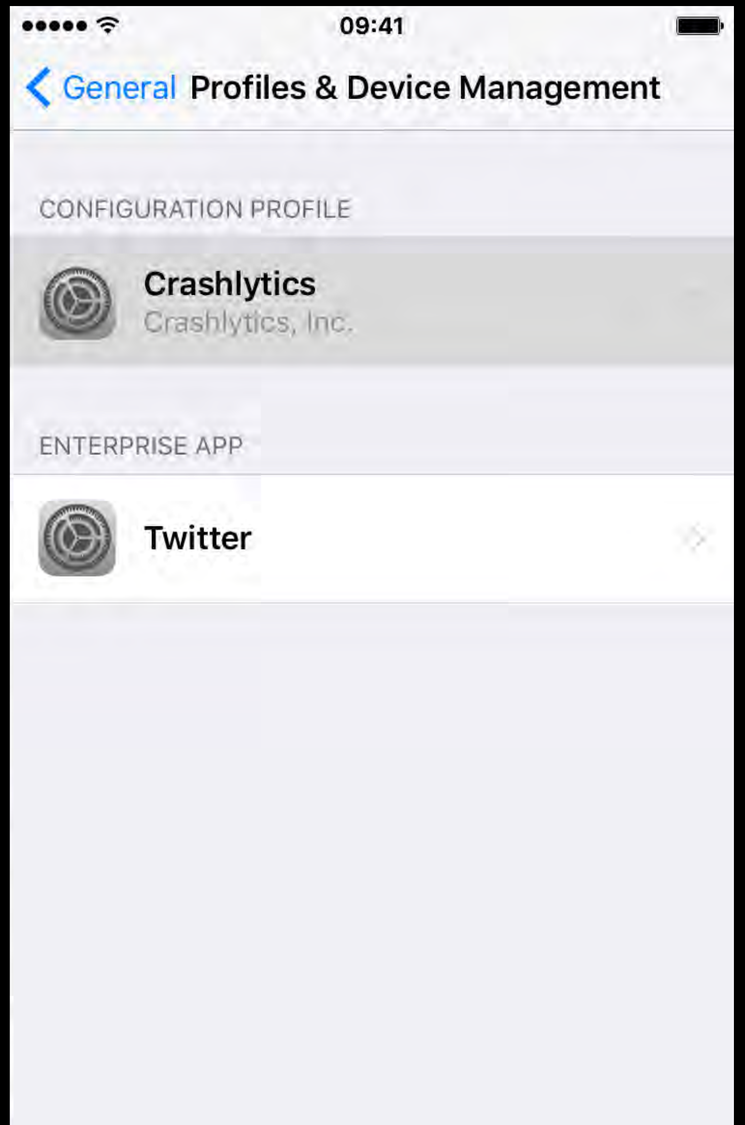
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadIdentifier</key>
    <string>com.acme.profile.wifi</string>
    <key>PayloadRemovalDisallowed</key>
    <true/>
    <key>PayloadScope</key>
    <string>System</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>48a39070-1e4c-0131-c321-000c2944c108</string>
    <key>PayloadOrganization</key>
    <string>ACME Inc.</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadDisplayName</key>
    <string>WiFi</string>
    […]
```

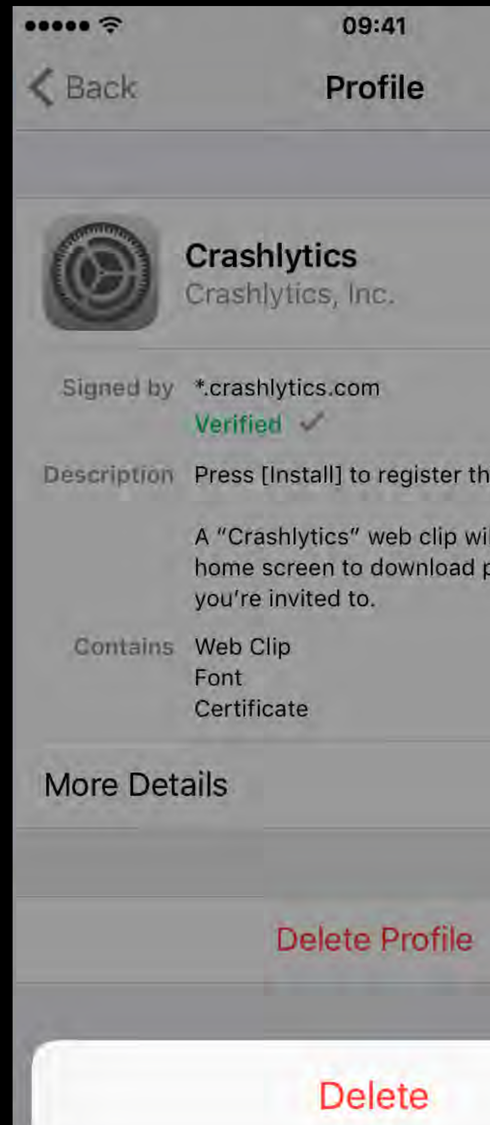


Configuration Profiles (contintued)

UNIVERSITY OF OXFORD

```
    <key>PayloadContent</key>
    <array>
    <dict>
        <key>PayloadType</key>
        <string>com.apple.wifi.managed</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadEnabled</key>
        <true/>
        <key>EncryptionType</key>
        <string>WPA</string>
        <key>SSID_STR</key>
        <string>ssid</string>
        <key>Password</key>
        <string>password</string>
        <key>HIDDEN_NETWORK</key>
        <false/>
        <key>AutoJoin</key>
        <true/>
        […]
    </dict>
    </array>
</dict></plist>
```

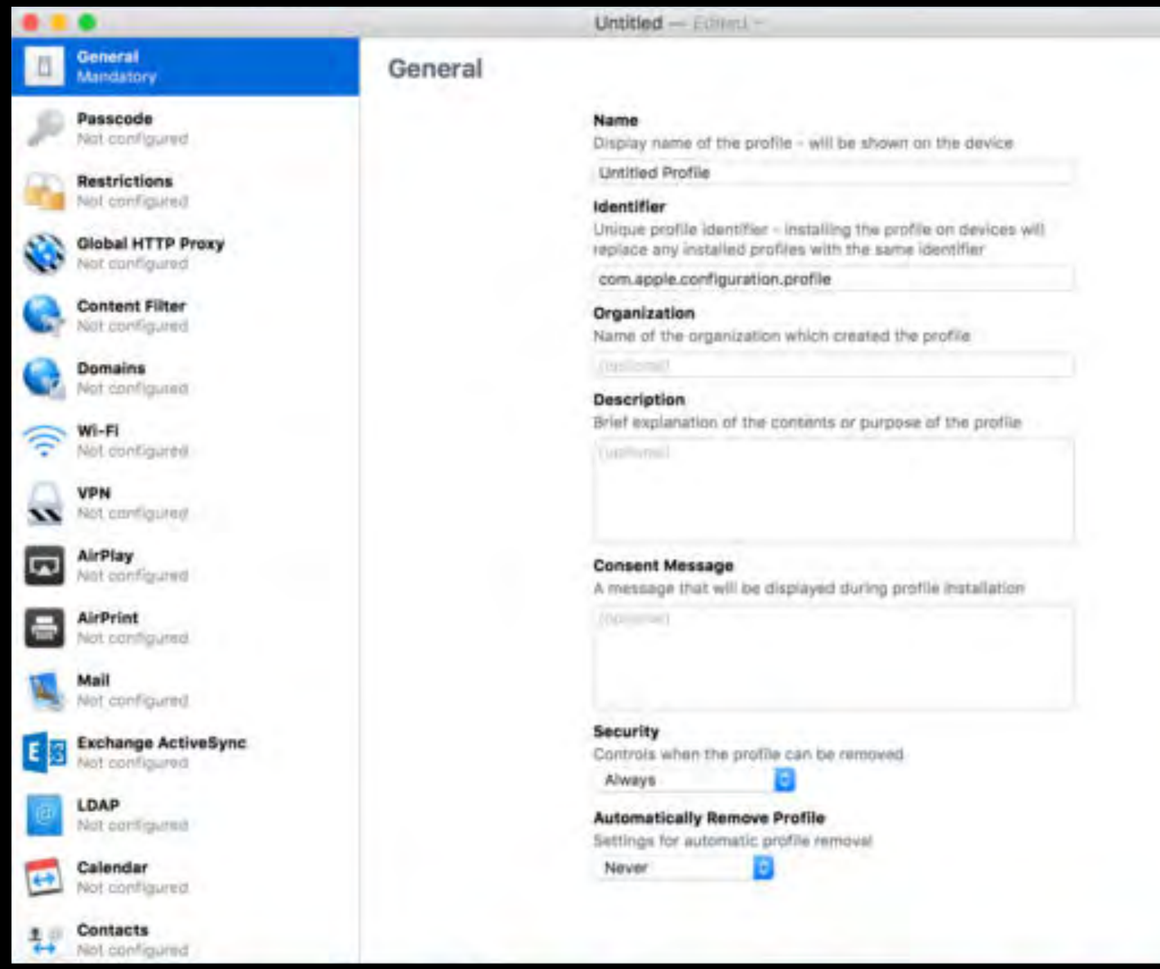




Deploying Configuration Profiles

UNIVERSITY OF OXFORD

- Using Apple Configurator (iOS only)
- In an email message
- On a webpage
- Using over-the air configuration
  using a Mobile Device Management Server
  (e.g. Apple OS X Server's Profile Manager)



Mobile Device Management

UNIVERSITY OF OXFORD

- Managed apps, books, domains, accounts, extensions, …
- Policy settings
- Security (e.g. encryption, passcodes, Touch ID, SSO)
- Remote control (e.g. selective remote wipe)
- Asset tracking
- Firmware / OS upgrades

Mobile Device Management for iOS

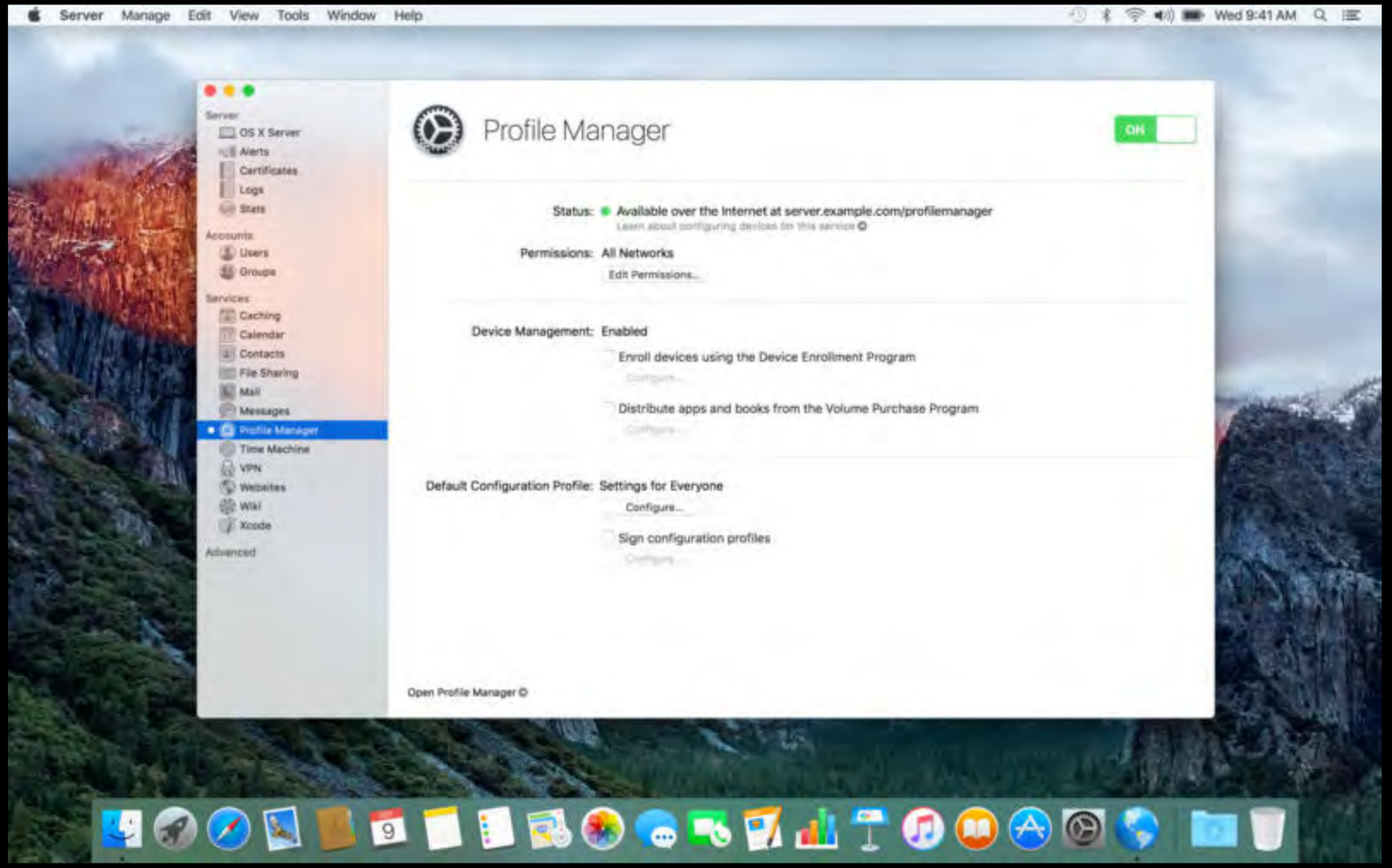
UNIVERSITY OF OXFORD

- Apple OS X Server Profile Manager
  https://www.apple.com/uk/support/osxserver/profilemanager/

- Hundreds of commercial on-premises and cloud offerings. €
  Comparison of MDM solutions at http://enterpriseios.com/
  - Airwatch €
    http://www.airwatch.com
  - Bushel €
    http://www.bushel.com
  - JAMF Casper Suite €
    http://www.jamfsoftware.com

Apple OS X Server

UNIVERSITY OF OXFORD

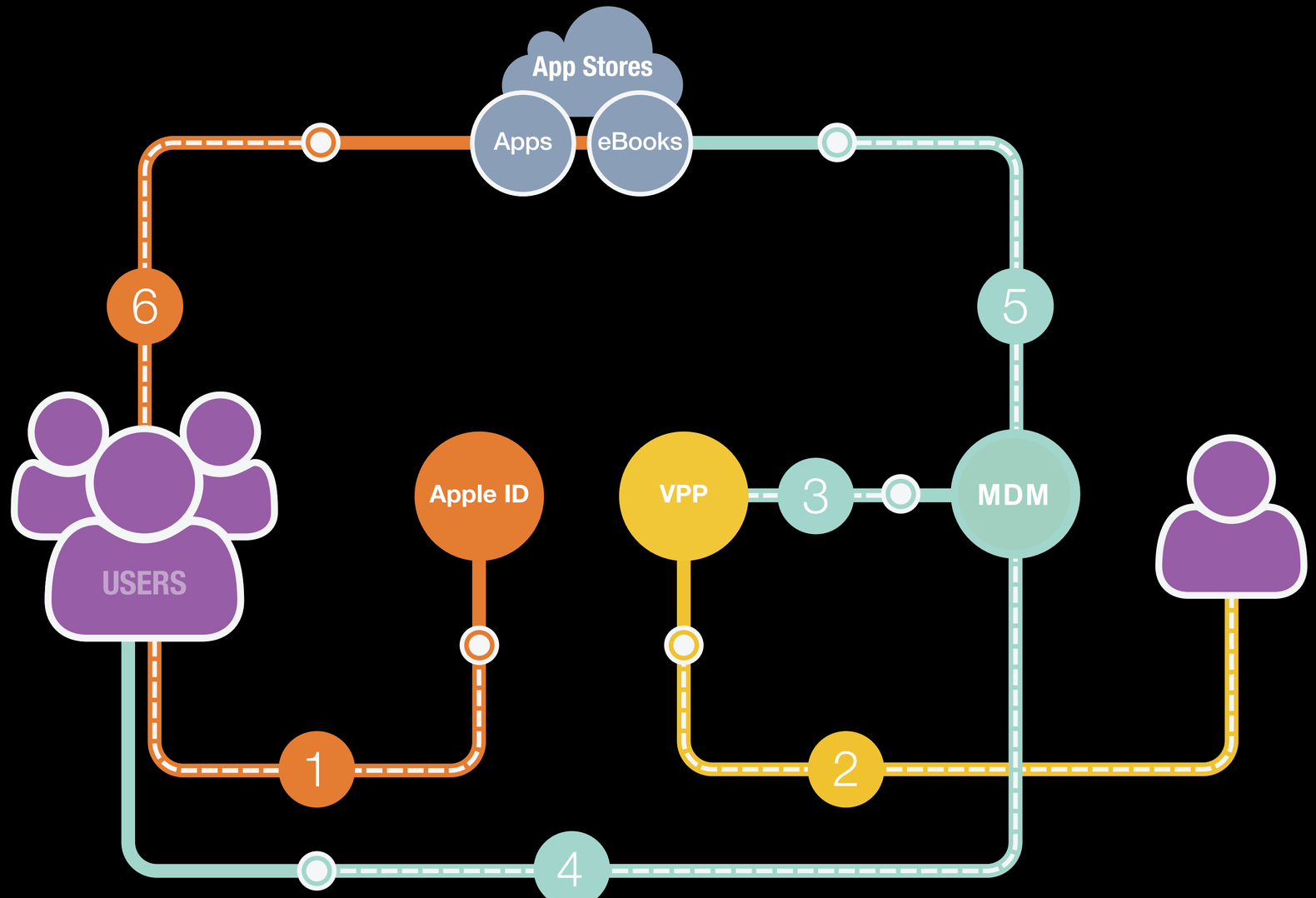


http://www.apple.com/de/osx/server/

Volume Purchase Program (VPP)

UNIVERSITY OF OXFORD

- Bulk purchase of apps and books
- Assign content to users or devices
- Deploy using MDM
- Revoke and re-assign
- Custom B2B apps for iOS



https://help.apple.com/deployment/programs/ http://images.apple.com/business/docs/VPP_Business_Guide.pdf

Orchard – iOS Management

UNIVERSITY OF OXFORD

Procure
to DEP enabled account

Ship
directly to user

DEP
automatic MDM enrollment

MDM
Profiles, remote commands

VPP
manage Apps, eBooks

'Zero Touch' Workflow


UNIVERSITY OF
OXFORD


UNIVERSITY OF
OXFORD

Linux Management Workflow

UNIVERSITY OF OXFORD

PXE Boot

Disk Partitioning

Bootstrapping

Packages

Configuration

OS X Management Workflow

UNIVERSITY OF OXFORD

PXE Boot

NetBoot,
NetInstall

Disk Partitioning

Bootstrapping

Imaging

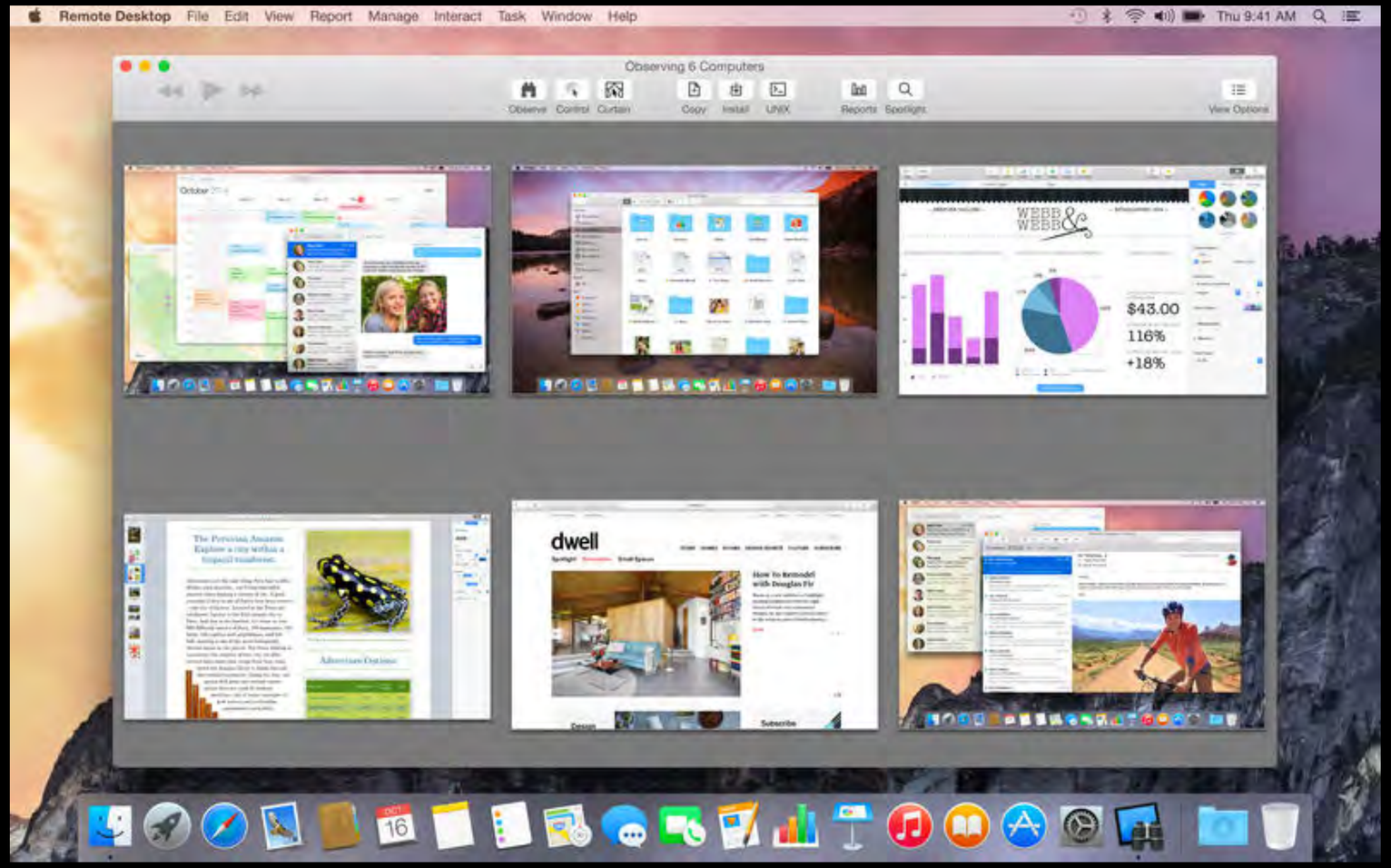
Packages

Configuration

Profiles,
MCX

Apple Remote Desktop

UNIVERSITY OF OXFORD



http://www.apple.com/de/remotedesktop/

Booting over the Network

UNIVERSITY OF OXFORD

- Apple BSDP – Boot Service Discovery Protocol

  http://www.opensource.apple.com/source/bootp/bootp-170/Documentation/BSDP.doc

  - BSDP may coexist with any DHCP service
  - OS X 10.11 adds security enhancements

    `csrutil netboot add <address>` – https://support.apple.com/en-gb/HT205054

- BSDP Implementations
  - Apple OS X Server NetInstall service
  - BSDPy - Python implementation of BSDP

    https://bitbucket.org/bruienne/bsdpy
  - ISC DHCPD, TFTP, HTTP-Server (e.g. Apache2, nginx)

- Justin Elliot: NetBoot Fundamentals and Customizations

  https://youtu.be/yKS2moLySi0

NetBoot Image Types

- **NetBoot** – Boot a server based OS X image
  - Diskless requires AFP or NFS share to store 'shadow' files
  - Hack the OS X image to use a RAMDisk instead

    https://www.afp548.com/2011/02/01/serving-diskless-netboot-for-your-macs-without-os-x-server/

- **NetInstall** – Boot an OS X installer

- **NetRestore** – Restore a volume using an `asr` disk image

Network Disk Image Creation

UNIVERSITY OF OXFORD

- Manual
  - Apple System Image Utility

    https://support.apple.com/en-gb/HT202652

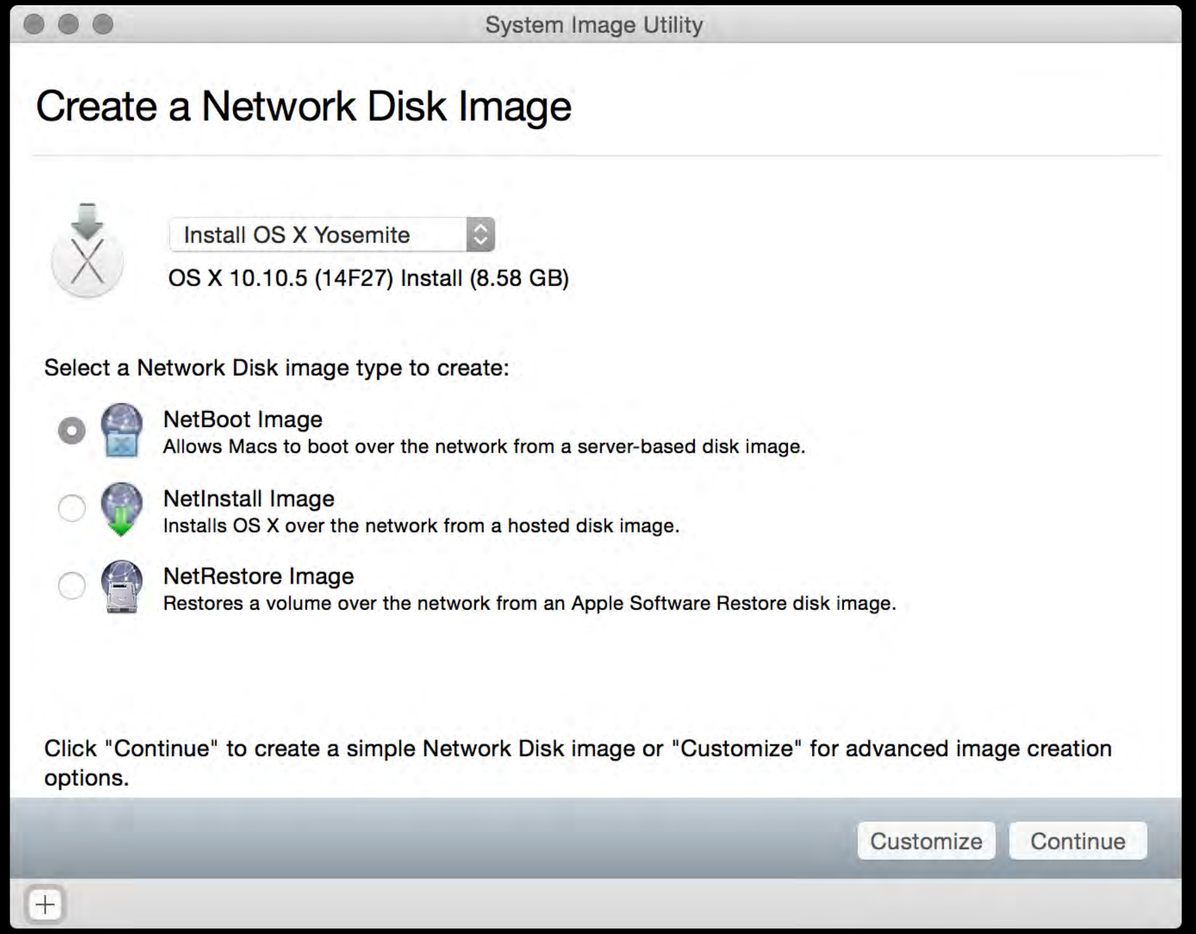
    https://support.apple.com/en-gb/HT202061
  - Casper NetInstall Image Creator

    https://github.com/jamf/CasperNetInstallCreator
  - AutoCasperNBI

    https://github.com/macmule/AutoCasperNBI/

- Scripted
  - AutoNBI.py

    https://bitbucket.org/bruienne/autonbi




Finder File Edit View Go Window Help
Wed 11:12 a.m.

Imaging Techniques

UNIVERSITY OF OXFORD

Thick Image

Hybrid Image

Thin Image

No Image

Source: http://technet.microsoft.com/en-us/library/ee956904(WS.10).aspx

Imaging Software

UNIVERSITY OF OXFORD

- Apple asr (and derived tools)
- Casper Imaging €
  www.jamfsoftware.com/products/casper-suite/
- DeployStudio
  http://www.deploystudio.com/
- Imagr
  https://github.com/grahamgilbert/imagr
- FileWave Imaging €
  https://www.filewave.com/products/imaging/
- LANrev (formerly known as Absolute Manage) €
  https://heatsoftware.com/lanrev/

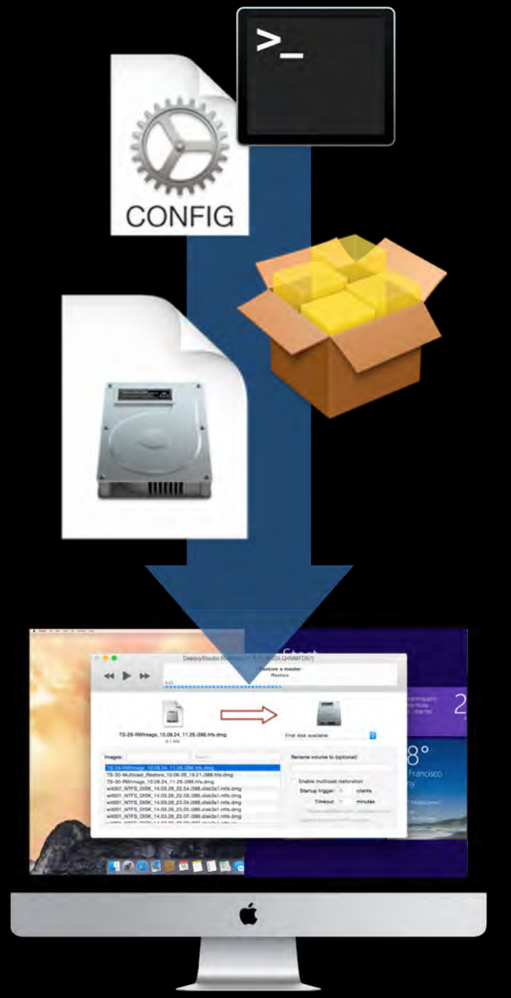
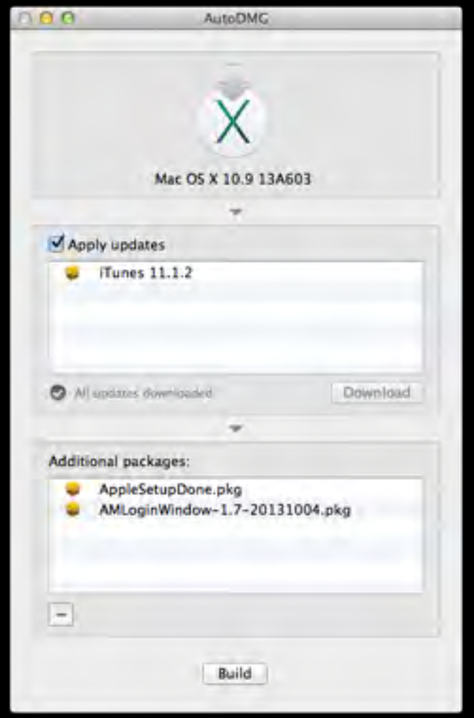
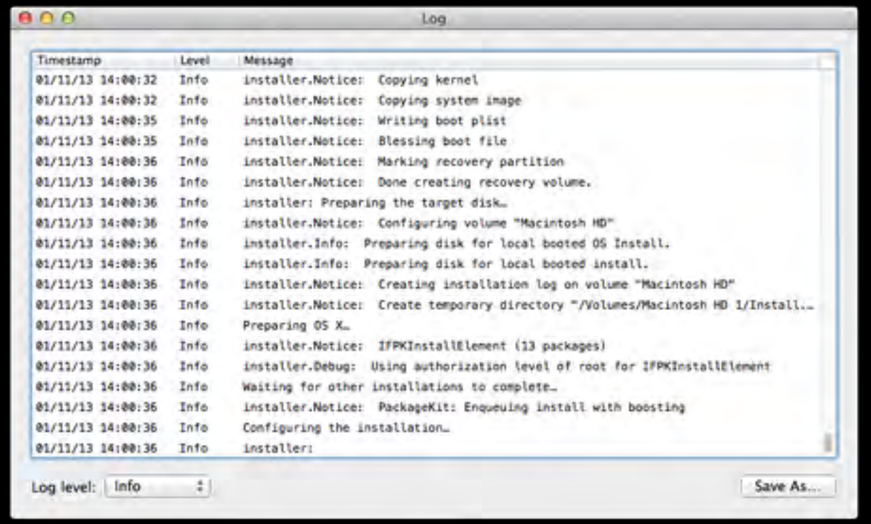


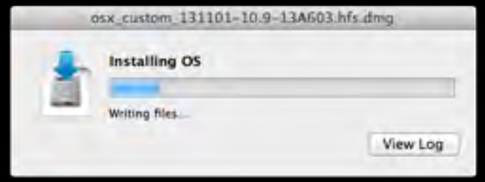
Image Creation

UNIVERSITY OF OXFORD

- Apple Disk Utility
  https://support.apple.com/en-gb/HT202841
- AutoDMG
  https://github.com/MagerValp/AutoDMG
- Casper Composer €
  www.jamfsoftware.com/products/casper-suite/
- FileWave Imaging €
  https://www.filewave.com/products/imaging/
- NBICreator (beta)
  https://github.com/NBICreator/NBICreator








Finder File Edit View Go Window Help
Wed 11:12 a.m.
SKYNET
CYBERDYNE
SYSTEMS

Inventory & Management

- Filewave €

  https://www.filewave.com/

- HEAT LANrev (formerly Absolute Manage) €

  https://heatsoftware.com/lanrev/

- JAMF Casper Suite €

  http://www.jamfsoftware.com/products/casper-suite/

- Microsoft System Center Configuration Manager (SSCM) €

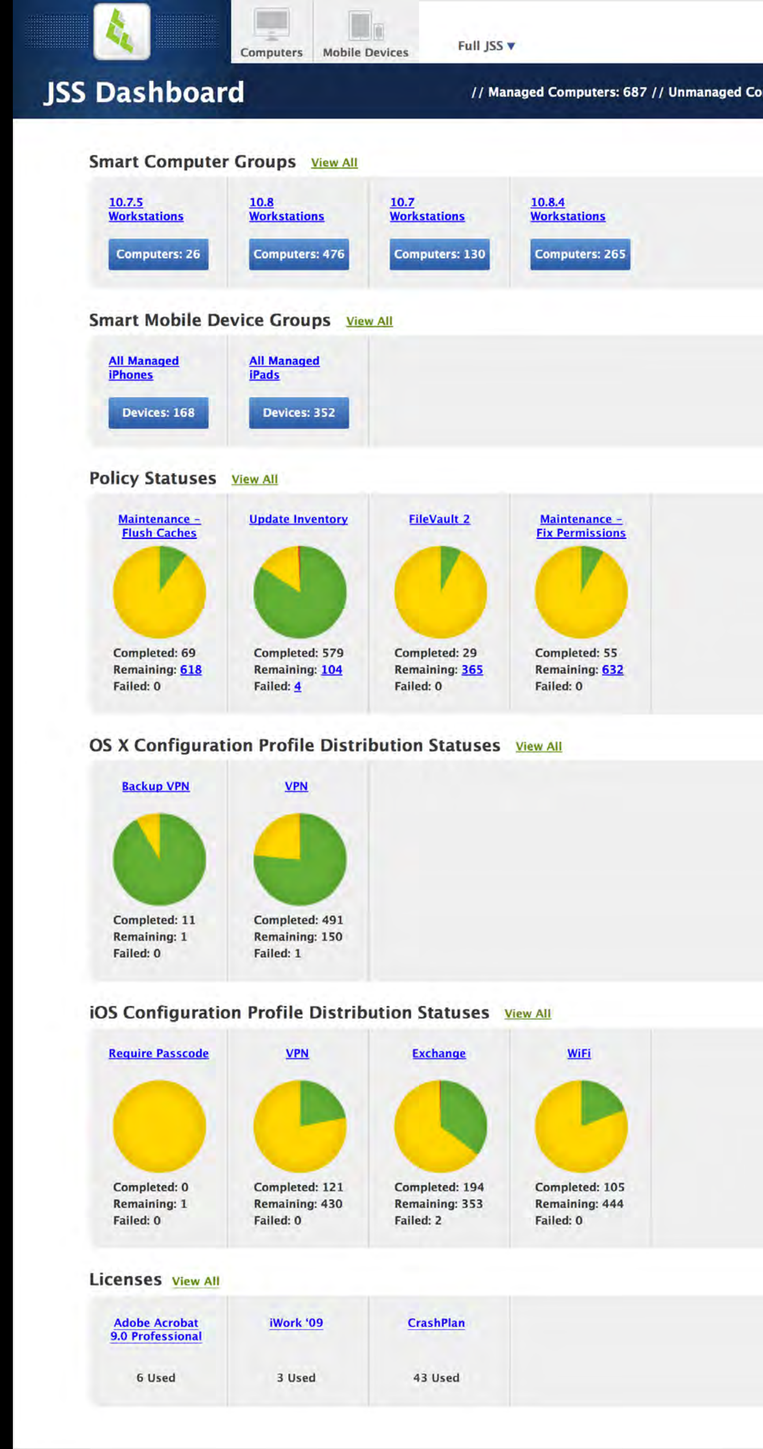
  https://www.microsoft.com/en/server-cloud/products/system-center-configuration-manager/

- SAL+ €

  http://salsoftware.com/

SAL

https://github.com/salsoftware/sal



Challenge: Applications

UNIVERSITY OF OXFORD

/Users/horst

/Users/horst/Applications

/Applications

The OS X platform lacks a package manager like apt, yum or zypper

Munki

https://github.com/munki/munki/wiki

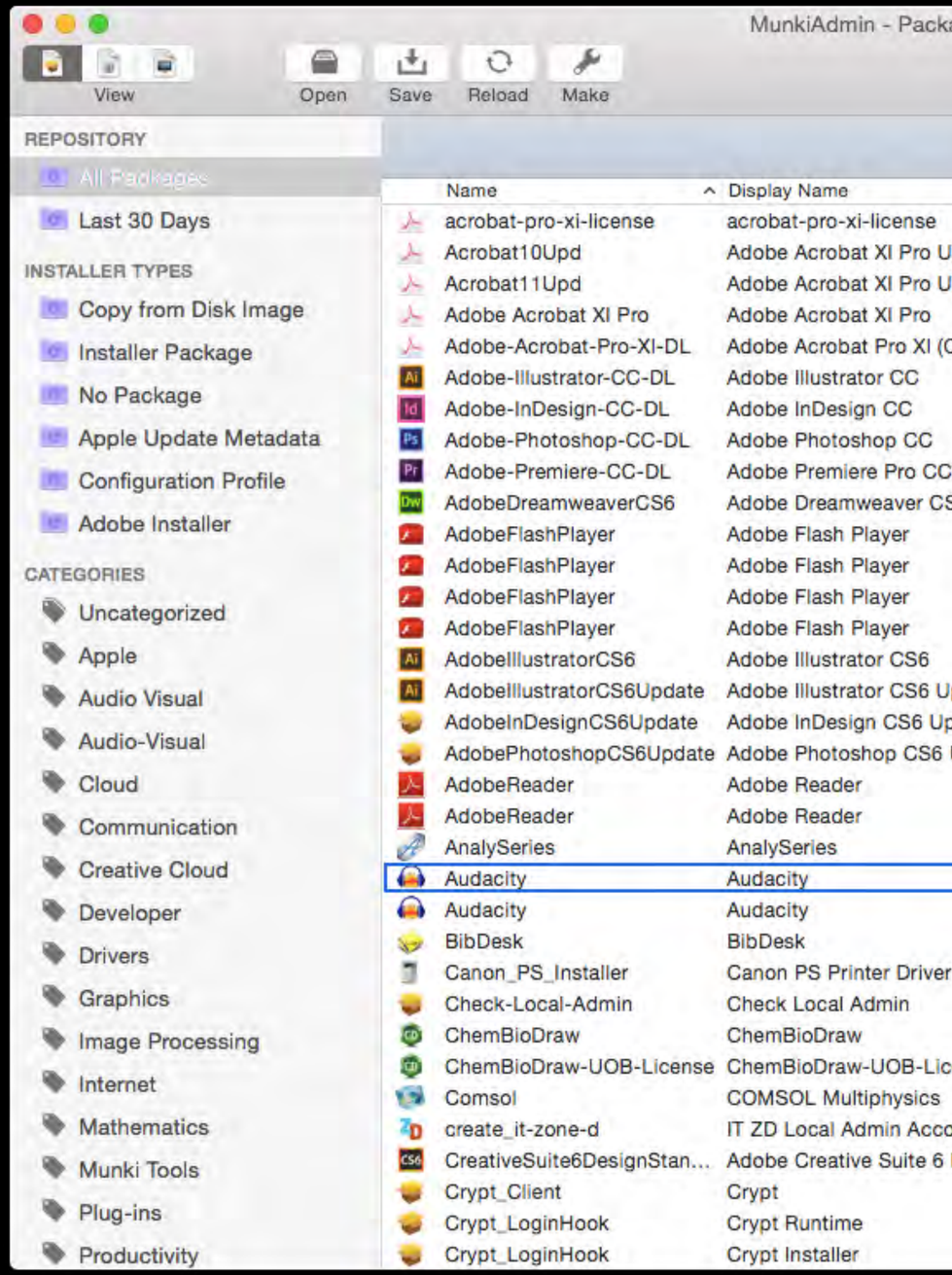
UNIVERSITY OF OXFORD

- System administrator friendly toolset
  - text based configuration
  - powerful command line tools
- Friendly user interface:
  Managed Software Center.app
- Excellent tool ecosystem
- MacSysadmin 2014 - G. Neagle:
  What's new with Munki?
  http://docs.macsysadmin.se/2014/2014doc.html

Munki Ecosystem

- MunkiAdmin https://github.com/hjuutilainen/munkiadmin
- SAL https://github.com/salsoftware/sal
- munkireport-php https://github.com/munkireport/munkireport-php
- MunkiWebAdmin https://github.com/munki/munkiwebadmin
- munki-staging https://github.com/ox-it/munki-staging
- Simian https://github.com/google/simian
- Manana https://github.com/ox-it/manana

and many many more https://github.com/timsutton/python-macadmin-tools#munki



AutoPkg

https://github.com/autopkg/autopkg

UNIVERSITY OF OXFORD

- Automated preparation of software for managed distribution
- Community maintained recipes (PropertyList XML) to automate complex tasks

  ```
  Firefox.download.recipe
  Firefox.pkg.recipe
  Firefox.munki.recipe
  ```

- Excellent integration with Munki
- Workflows for other management tools like Absolute Manage, JAMF Casper Suite
- Recipe Robot

  https://github.com/homebysix/recipe-robot
- MacSysadmin 2014- G. Neagle, T. Sutton

  AutoPkg: Crowd-sourcing Mac packaging and deployment

  http://docs.macsysadmin.se/2014/2014doc.html

Challenge: OS X Releases

UNIVERSITY OF OXFORD

OS X Yosemite release history

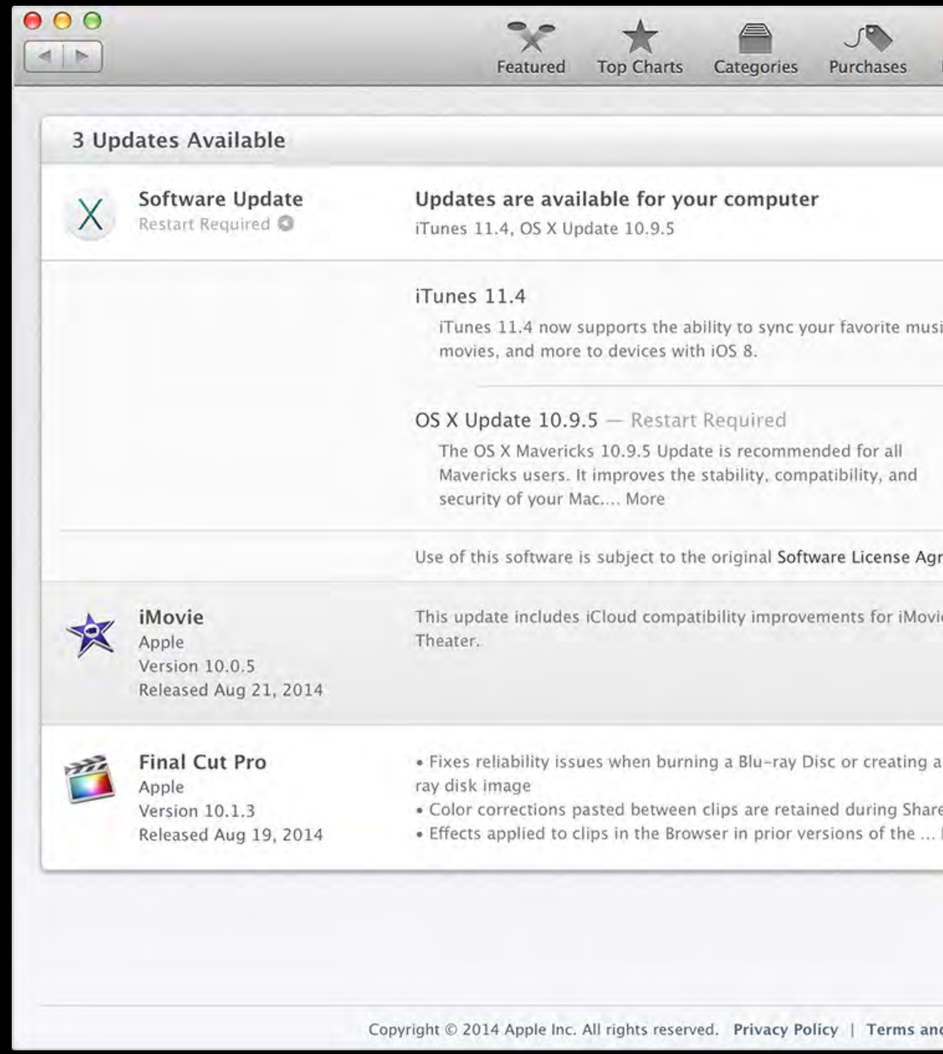
UNIVERSITY OF OXFORD

10.10.5	14F1509	
10.10.4	14E46	
10.10.3	14D131	14D136
10.10.2	14C109	14C1510, 14C1514, 14C2043, 14C2513
10.10.1	14B25	
10.10	14A389	

Solution: In-Place Upgrades

UNIVERSITY OF OXFORD

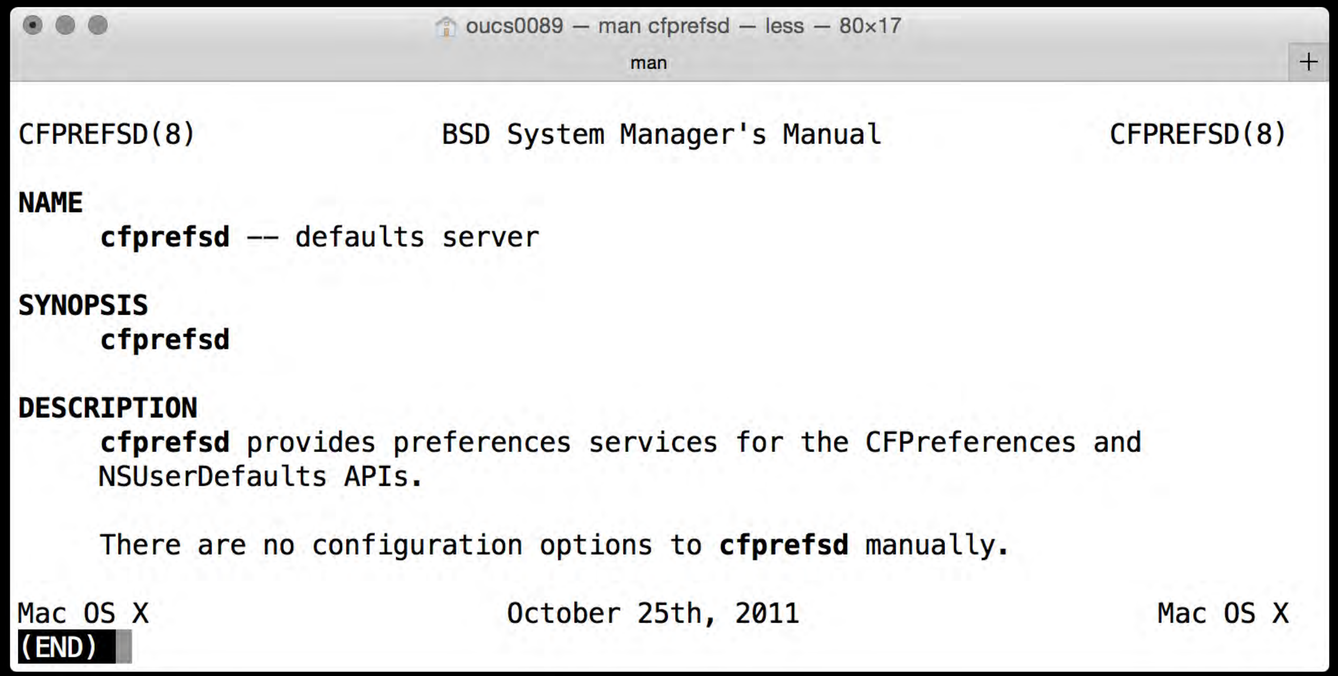
- Minor version updates:
  - Apple Software Update based workflows
- Software Update Servers:
  - Apple SUS as part of Server
  - Reposado
    https://github.com/wdas/reposado
  - Margarita
    https://github.com/jessepeterson/margarita
- Major version updates:
  - All commercial management suites provide workflows
  - createOSXinstallPkg
    https://github.com/munki/createOSXinstallPkg



Challenge: Configuration

UNIVERSITY OF OXFORD

- Several configuration methods
  - defaults / plists
  - MCX
  - Profiles
  - proprietary (files, databases)
- Configuration caching using cprefsd (introduced 10.9)



Solution: Configuration Management

- Profiles & MDM
- Configuration management tools:
  - chef
    https://www.chef.io/chef/
  - puppet
    https://puppetlabs.com/puppet/puppet-open-source
- Munki: scripts in combination with (payload free) packages
  - idempotency
  - use Apple tools whereas possible
- All commercial management suites provide workflows €

Mobile Device Management for OS X

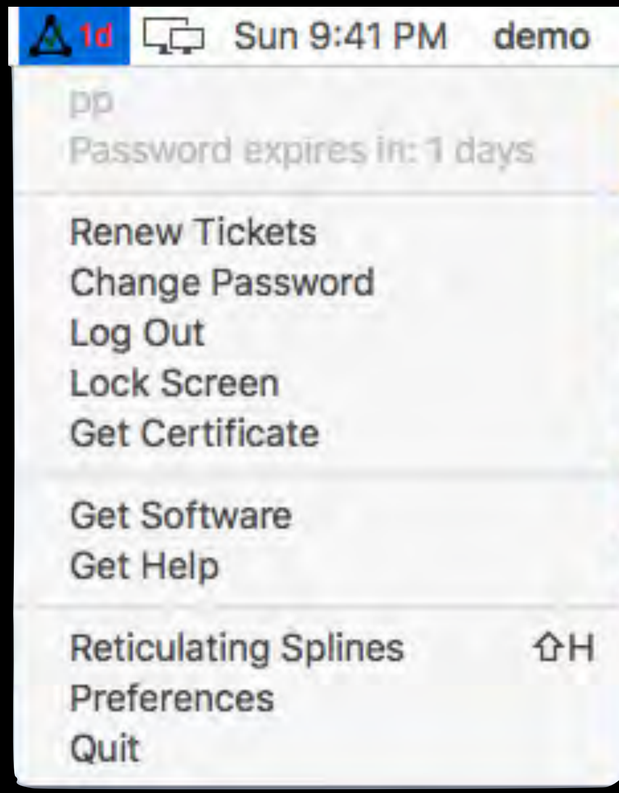
UNIVERSITY OF OXFORD

- Apple OS X Server – Profile Manager
  https://www.apple.com/uk/support/osxserver/profilemanager/
- Hundreds of commercial on-premises and cloud offerings. €
  Comparison of MDM solutions at http://enterpriseios.com/
- coMmanDMent
  https://github.com/jessepeterson/commandment
- microMDM
  https://micromdm.io/
- mdmvendorsign - CSR for Apple's MDM push service
  https://github.com/grinich/mdmvendorsign

Authentication & Authorisation

UNIVERSITY OF OXFORD

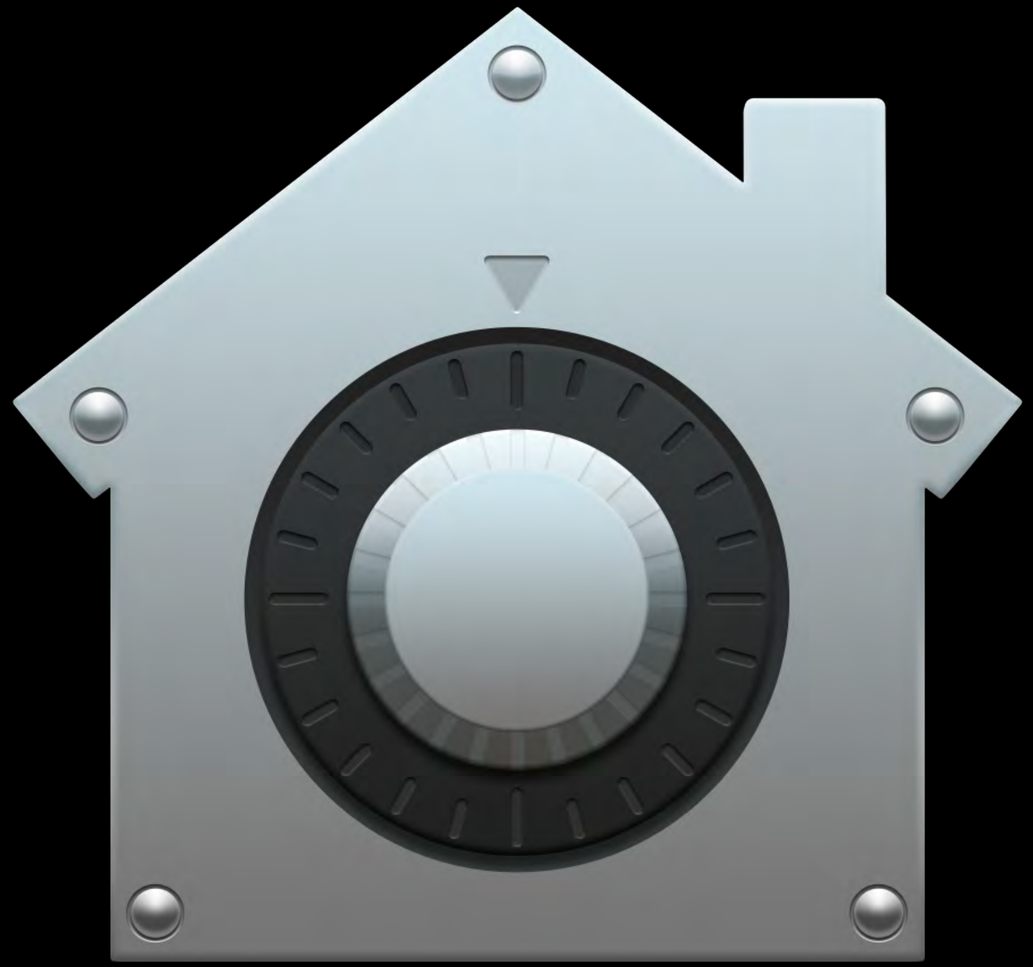
- Built-in Active Directory client
  - (restricted) AD support
  - 'mobile' accounts
- Apple Enterprise Connect $ (US only)
- NoMAD – the best of AD without binding to it
  "NoMAD allows for all of the functionality you would want from a Mac bound to Active Directory without having to actually bind to AD."
  https://gitlab.com/Mactroll/NoMAD/
- KerbMinder – automatically refresh Kerberos tickets
  https://github.com/pmbuko/KerbMinder



Encryption: FileVault2

UNIVERSITY OF OXFORD

- Require & enforce FileVault2 (via Profile)
- Recovery key escrow solutions
  - Cauliflower Vest
    https://github.com/google/cauliflowervest
  - Crypt
    https://github.com/grahamgilbert/Crypt
  - Most commercial management suites €



Security: More Useful Tools

UNIVERSITY OF OXFORD

- osquery – endpoint visibility
  https://osquery.io/
- Plan B – remediation for managed Macs
  https://github.com/google/macops-planb
- Santa – binary whitelisting/blacklisting system
  https://github.com/google/santa
- Zentral – Elastic search based infrastructure event handler
  https://github.com/zentralopensource/zentral

Orchard – OS X Management

UNIVERSITY OF OXFORD


DEP


MDM


Profiles


AD Binding


VPP


Munki

Branding


Non-App Store


Updates

NetBoot & Imaging

Key Lessons Learned

UNIVERSITY OF OXFORD

- Trust your users – don't be the evil BOFH
- Automate yourself out of your job ;)
- Never fight against Apple's tools and workflows
  - Follow the official deployment references
  - Use the Device Enrollment Program
  - Use the App Store (and VPP)
- Don't be afraid to ask for help – join the Mac admin community on Slack

  http://macadmins.org

Official References

UNIVERSITY OF OXFORD

iOS Deployment Reference

http://help.apple.com/deployment/ios/

OS X Deployment Reference

http://help.apple.com/deployment/osx/

Apple Developer Program

http://developer.apple.com

Vielen Dank!

https://github.com/mjung/publications

Marko Jung

Galactic Viceroy of Research Excellence

m@mju.ng @mjung fb.com/markohjung

http://mju.ng/give